IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE-BCM **ORAL ARGUMENT REQUESTED**

REPLY MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE AMENDED COMPLAINT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

REGULATIONS

OTHER AUTHORITIES

PRELIMINARY STATEMENT

The SEC continues to do in its opposition what it has done from the start of this matter: It advances unsupportable legal theories; it leaps to unwarranted conclusions from documents it either misunderstands or willfully mischaracterizes; it stretches the law and facts however it can to fit a predetermined narrative. The SEC's aim has been apparent since its investigation began. It is intent on using this case as a high-profile litigation vehicle—with SUNBURST as eye-catching background—to try to *expand* (not enforce) disclosure requirements as they relate to cybersecurity, and to claim a mandate for regulating cybersecurity controls that it does not have. The Court should put an end to this ill-conceived project and dismiss the lawsuit in its entirety.

The SEC still offers no coherent theory as to how the Company's investor filings could have been fraudulent. It argues that SolarWinds' cybersecurity risk disclosure should have used different language or included more details; but the bottom line is that the disclosure contained no misleading statement, without which there can be no fraud. Nor can the SEC plausibly allege that the December 2020 8-K hid the "true risk" of SUNBURST, given that it described a cataclysmic cybersecurity incident exposing up to 18,000 customers to potential compromise—a point to which the SEC offers no meaningful rebuttal.

With no plausible allegations based on the Company's disclosures, the SEC is left trying to allege some sort of misrepresentation in the Company's Security Statement—but it does so only by misportraying or ignoring the very documents on which it relies. The SEC makes no attempt to substantively address the conflicts between its allegations and the cited documents, instead seeking to avoid the issue by characterizing the conflicts as factual disputes. But, having staked its case on these documents, the SEC cannot disregard what they actually say. Even on a motion to dismiss, the incorporated documents control. And those documents show that the SEC's otherwise conclusory allegations of "pervasive" failures deserve no credit.

As to scienter, the SEC abandons its fanciful theory that Mr. Brown hatched an intentional scheme to lie about SolarWinds' cybersecurity to "obtain and retain business," retreating to argue only that Mr. Brown knew of security deficiencies. But as the incorporated documents show, the SEC does not plausibly allege—let alone establish a "strong inference"—that Mr. Brown believed SolarWinds was pervasively failing to implement any policies in the Security Statement. And as to statements in the Company's public filings, as a matter of law, Mr. Brown's knowledge cannot provide a basis for liability, especially for the risk disclosure, which he did not allegedly review.

The SEC's attempts to rescue its controls violation claims also fail. Notwithstanding its efforts to second-guess the application of SolarWinds' disclosure controls in hindsight, the SEC does not contest that those controls were reasonably designed, which is all the relevant rule requires. And the SEC continues to grossly misread the internal accounting controls statute by construing it to apply to broadly encompass cybersecurity controls with no nexus to accounting.

This case should never have been brought. The Court should not allow it to proceed further.

ARGUMENT

I. The Fraud and False-Filing Claims Should Be Dismissed

A. The SEC Fails to Allege a Material Misrepresentation or Omission

1. The Risk Disclosure Was Not Materially Misleading

The SEC contends that SolarWinds' risk disclosure was misleading because SolarWinds supposedly had an independent "disclosure duty," Opp. 24, to divulge "specific" details about its allegedly "poor cybersecurity posture." Opp. 25. To begin with, no such duty existed (even if the SEC's allegations about the Company's cybersecurity were true, which they are not). As Defendants previously explained, Regulation S-K requires companies to disclose only the "most significant" risks to their businesses, *Modernization of Regulation S-K Items 101, 103, and 105*, Rel. No. 34-89670, 2020 WL 5076727, at *29 (SEC Aug. 26, 2020), "[c]oncisely" and "in plain

English," 17 C.F.R. § 229.105—which is exactly what SolarWinds did in warning that, despite its security measures, it was vulnerable to a cyberattack and the attendant material consequences. Nothing required SolarWinds' risk disclosure to speak to any details beyond that.[1] To the contrary, as Defendants have pointed out, SEC guidance during the Relevant Period specifically reassured companies they did *not* need to make "detailed disclosures that could compromise [their] cybersecurity efforts," Mot. 14, as disclosing details about cybersecurity vulnerabilities would do.[2]

In any event, even if there *were* such a duty, the mere omission of information required by that duty would not render SolarWinds' risk disclosure fraudulent. The SEC's argument based on a purported disclosure duty is the kind of "pure omission" theory of securities fraud that the Supreme Court recently made clear is not valid. *See Macquarie Infrastructure Corp. v. Moab Partners, L.P.*, 144 S.Ct. 885, 891-92 (2024). As *Macquarie* holds, even if a duty to disclose exists, an omissions theory under Section 10(b) "requires identifying affirmative assertions (*i.e.*, 'statements made') before determining if other facts are needed to make those statements 'not misleading.'" *Id.* at 891. The SEC's allegations fail that requirement: The statement made—that SolarWinds was vulnerable despite its security measures—was not rendered misleading by allegedly omitting details about vulnerabilities or deficient security measures. *See In re Union Carbide Class Action Sec. Litig.*, 648 F.Supp. 1322, 1324-26 (S.D.N.Y. 1986) (registration

[1] Indeed, even if the Company's disclosures were "generic"—which SolarWinds disputes—the guidance the SEC cites discourages generic disclosures primarily because they "contribute to the increased length" of SEC filings—not, as the SEC now insinuates, because making disclosures "similar to those used by others in their industry" is somehow false or misleading. 2020 WL 5076727, at *29.

[2] The SEC tries to wave away the security implications of requiring companies to disclose specific information about their cybersecurity vulnerabilities, asserting that only a "categorical assessment of those issues" needs to be provided. Opp. 30. But that is what SolarWinds' risk disclosure *did* provide: a categorical statement that it was "vulnerable." The SEC argues that companies must go further and disclose things like "significant deficiencies in access controls," *id.*, but such information by itself is useful to, and a lure for, attackers (like a sign outside a house suggesting that there are weak locks on the doors). And the SEC offers no principled reason to draw the line at "access controls," as opposed to requiring companies to disclose *all* their cybersecurity deficiencies—which would provide nothing less than an initial reconnaissance report to hackers seeking potential weaknesses.

statement not fraudulent despite undisclosed "major safety defects" creating "higher potential for a serious accident," because complaint failed "to identify any statement contained in [the] registration statement made misleading by [the] omission").

The SEC still offers no consistent, articulable theory of how the risk disclosure was supposedly misleading or what exactly SolarWinds should have disclosed instead. It says that "the issue is not whether [SolarWinds] paired the modifier 'very' with the word 'vulnerable,'" Opp. 26, but in the same breath it criticizes SolarWinds for not disclosing that its "*critical* assets" were "*highly* vulnerable." *Id.* at 26-27 (emphasis added). Similarly, the SEC says it "is not asserting that each specific cybersecurity problem recited in the Amended Complaint needed to be individually disclosed," Opp. 30, but simultaneously criticizes the "[t]he omission of any reference to the Company-specific cybersecurity problems," "such as … significant deficiencies in access controls," Opp. 26-27. The SEC is grasping for an intelligible theory where there is none. "Disclosure is not a 'rite of confession or exercise of common law pleading.'" *In re Morgan Stanley Info. Fund Sec. Litig.*, 592 F.3d 347, 365 (2d Cir. 2010). SolarWinds categorically disclosed that its "software" and "systems" were "vulnerable" to cyberattack. That was true—and that was enough. The disclosure did not need to be adorned with any particular words, or references to any particular cybersecurity problems, for it not to be misleading.

The SEC's effort to distinguish SolarWinds' case law is unavailing. It tries to distinguish *In re Qudian* and *In re Equifax*, for example, by arguing that SolarWinds' disclosure was "generic" and "fail[ed] to disclose specific, known 'facts'" about supposed cybersecurity deficiencies. Opp. 27. But SolarWinds' disclosure was no more "generic" than the one in *Qudian*. *See* 2019 WL 4735376, at *8 (S.D.N.Y. Sept. 27, 2019). And that case *also* involved extensive allegations, like those here, that the defendant "failed to disclose that the Company lacked adequate data security

controls." Complaint at ¶¶ 78-82, *In re Quidian Inc. Sec. Litig.*, No. 17-cv-9741 (S.D.N.Y. July 27, 2018), ECF No. 134 (alleging that, despite touting customer data protections, defendant had "extremely lax internal controls and poor security procedures over client information and no effective data protection policy"). Similarly, in *Equifax*, the defendant's disclosure broadly warned that "[d]espite" its "security measures," it "could be vulnerable" to attack, while allegedly failing to disclose known vulnerabilities such as "[im]proper network monitoring." 357 F.Supp.3d 1189, 1225-26 (N.D. Ga. 2019). Both cases are on all fours with this one, and both found the relevant disclosure unactionable because it did not contain any misleading statements—just like SolarWinds' disclosure here.

The cases offered by the SEC to support its position do not do so, as they involved affirmative misstatements made in risk disclosures. Thus, in *Meyer v. Jinkosolar Holdings Co., Ltd.*, the defendant's prospectus asserted it had "pollution-preventing equipment and 24–hour monitoring teams" in place, but omitted that the equipment and teams were "failing to prevent serious ongoing pollution problems," 761 F.3d 245, 250-51 (2d Cir. 2014). Likewise, in *Fannie Mae*, the defendant made detailed assertions to the effect that it had "a strong risk-management program," which were allegedly untrue. *In re Fannie Mae 2008 Sec. Litig.*, 742 F.Supp.2d 382, 405-06 (S.D.N.Y. 2010). These cases are inapposite because SolarWinds' risk disclosure did not contain *any* affirmative statement about its security controls, let alone one that was misleading.[3]

The SEC also cites cases in which the defendant was allegedly aware that the specific risk the disclosure warned about had already materialized, but failed to disclose that fact. *See SEC v. DeFrancesco*, 2023 WL 4631449, at *4 (S.D.N.Y. July 20, 2023); *Holding N.V. Sec. Litig.*, 405

[3] The SEC also cites *In re BP P.L.C. Securities Litigation*, but that case simply cites back to *Fannie Mae*, and actually *rejected* the claim that the defendant "misrepresented its exposure to risk by failing to disclose that it was unprepared to contain an oil leak." 843 F.Supp.2d 712, 760-61 (S.D. Tex. 2012).

F.Supp.2d 388, 400 (S.D.N.Y. 2005). Those cases too are inapposite: Here, the risk disclosed was the potential for a material cyberattack, and the SEC does not allege that SolarWinds knew that a material cyberattack already occurred before learning of SUNBURST. *See In re Equifax*, 357 F.Supp.3d at 1227 (distinguishing *Van der Moolen* on similar grounds). Indeed, the SEC explicitly disclaims such a theory. *See* Hr'g Tr. 5:17-24, Dec. 14, 2023, ECF No. 32 (acknowledging at initial conference that this case is different from "previous [SEC] cases where there was a cybersecurity incident or breach that was not necessarily disclosed in a timely fashion …. [O]nce SolarWinds became aware of the breach, they did quickly make a disclosure."); Opp. 33-34 (distinguishing certain cases because they "involved allegations [of misstatements] premised on the fact of a breach," whereas the SEC's theory is based on allegedly deficient practices apart from any breach).

Failing to identify any affirmative misstatement in the risk disclosure, the SEC makes the remarkable assertion that the risk disclosure "essentially incorporate[d] the Security Statement." Opp. 33. Putting aside that the Security Statement was not misleading, *see infra* § I.A.3, it was not even mentioned, let alone incorporated, in the risk disclosure. *See In re Marsh & Mclennan Cos., Inc. Sec. Litig.*, 501 F.Supp.2d 452, 469 (S.D.N.Y. 2006) (explaining that alleged omissions must be "sufficiently connected to Defendants' existing disclosures to make *those* public statements misleading" (emphasis added)). The only reference in the risk disclosure to SolarWinds' security measures was the statement that SolarWinds was vulnerable to cyberattack "despite" those measures. That is, the disclosure warned investors that *whatever* measures SolarWinds might have in place—whether described in the Security Statement or not—investors should not rely on those measures to prevent a cyberattack. The effect of this language with respect to the Security Statement was to render it immaterial, not incorporate it. *See* Mot. 33-34.

2. The SUNBURST Disclosure Was Not Materially Misleading

The SEC's falsity arguments as to the 8-K fail as well. The SEC suggests there is a "factual

issue" over whether the 8-K's references to "successfully exploit[ing]" SUNBURST referred to the attacker "infiltrating [customer] networks" or, as the SEC believes, merely "inserting malicious code that could be used to infiltrate networks later." Opp. 34-35. But there is no factual issue; context makes clear the reference was to the former, not the latter. The 8-K specifically disclosed that numerous customers (up to 18,000) had installed an infected version of Orion—*i.e.*, a version of the software into which malicious code (SUNBURST) had been "inserted" that could later be used to infiltrate the customer's network. Obviously, the Company was not claiming to still be investigating whether *that* had occurred. Rather, the only sensible reading of the Company's statement—that it was still investigating whether SUNBURST had been "successfully exploited" as a "point of infiltration"—is that it was referring to whether the attacker had actually *used* SUBURST to successfully infiltrate a customer's network. The SEC alleges no facts sufficient to show that Mr. Brown had concluded by the time of the 8-K that any such infiltration had occurred, at USTP, PAN, or otherwise. And even if Mr. Brown *had* drawn that conclusion, SolarWinds *as a company* could have still wanted to investigate the issue more thoroughly, with the help of an outside forensics firm—as the 8-K said it was doing. For these reasons, the SEC has failed to plausibly allege the statements at issue were false. Mot. 18-19.[4]

More fundamentally, the SEC still fails to explain how this issue is plausibly material. The 8-K transparently disclosed that SUNBURST was believed to be the work of a state-sponsored actor, that it had been live since March 2020, that up to *18,000* customers had installed a version of Orion containing it, and that SolarWinds faced "numerous financial, legal, reputational and

[4] The SEC mischaracterizes Defendants' position in suggesting these arguments were aimed at showing lack of falsity as to the 8-K's statement that SUNBURST "could potentially allow an attacker to compromise the server on which the Orion products run." Opp. 35. Defendants' brief separately explained that this other statement was not adequately alleged to be false because, even if SUNBURST was present on a customer's system, that did not necessarily mean that the attacker could access it. Mot. 17. The SEC's opposition fails to address—and hence concedes—that separate argument.

other risks" as a result. Mot. 20-21. It defies common sense to believe that a reasonable investor, knowing all this, would choose to hold onto their SolarWinds stock, but would have made a different decision if only they had been told that, out of these 18,000 customers, *two* were supposedly known to have been "infiltrated." Given the large universe of affected customers and the sophistication of the threat actor, a reasonable investor would independently assume that many *more* than two customers were likely infiltrated. Indeed, the 8-K itself noted there were "many" media reports attributing attacks "on U.S. government agencies and other companies" to SUNBURST—so investors knew this was more than a "theoretical" possibility.

"[A]lleged omissions must be evaluated by considering representations and omissions 'together and in context,'" and here the extensive disclosures about the seriousness of the incident make the purported omissions immaterial. *In re Bank of Am. AIG Disclosure Sec. Litig.*, 980 F.Supp.2d 564, 577-78 (S.D.N.Y. 2013) (finding alleged omission about particular lawsuit against defendant immaterial because it was "only one piece of the potential litigation [defendant] faced as a result of its exposure to [a particular] market" and "[t]he magnitude and risk of that potential exposure was extensively disclosed"), *aff'd*, 566 F.App'x 93 (2d Cir. 2014). The SEC's opposition makes no effort to address this key point—and thus must be deemed to have conceded it. *See, e.g.*, *In re UBS AG Sec. Litig.*, 2012 WL 4471265, at *11 (S.D.N.Y. Sept. 28, 2012) (a party "concedes through silence" when it fails to address opponent's arguments).[5]

3. The Security Policy Statements Were Not Materially Misleading

The SEC makes no real effort to grapple with the contradictions Defendants identified between the AC's allegations about the Security Statement and the actual documents it relies on;

[5] The SEC contests only the issue of comparative stock price movements after the December 2020 8-K versus the January 2021 8-K, arguing that materiality involves more than stock movement alone. Opp. 36. Defendants never suggested otherwise, but merely noted that the contrast in stock movements "confirms" the point that the first 8-K made the gravity of the situation clear and that the two incidents disclosed in the later 8-K were immaterial by comparison. Mot. 21. The SEC does not address that underlying point.

instead, it tries to write off these pleading deficiencies as factual disputes. But a plaintiff cannot "cherry-pick[]" bits of documents they like, yet "choose[] to ignore" the bits that undercut their claims. *Lopez v. Ctpartners Exec. Search Inc.*, 173 F.Supp.3d 12, 41 (S.D.N.Y. 2016) (Engelmayer, J.). Rather, a court is fully entitled at the dismissal stage to consider documents incorporated into the complaint by reference—including "for the truth of their contents." *Ark. Pub. Emps. Ret. Sys. v. Bristol-Myers Squibb Co.*, 28 F.4th 343, 352 n.3 (2d Cir. 2022); *see also In re DraftKings Inc. Sec. Litig.*, 650 F.Supp.3d 120, 175 (S.D.N.Y. 2023) (Engelmayer, J.) (rejecting scienter allegations about stock sales where they were contradicted by referenced documents). While "reasonable inference[s]" from "well-pleaded" allegations must be drawn in a plaintiff's favor, *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009), the SEC's allegations, when considered alongside the documents it relies on, are *not* well-pleaded, and the inferences it seeks are *not* reasonable. *See Kardovich v. Pfizer*, Inc., 97 F.Supp.3d 131, 140-41 (E.D.N.Y. 2015) (where plaintiff relies on incorporated documents that fail to show falsity, dismissal is appropriate because such deficiencies "go to the very heart of the plausibility standard under *Iqbal*, and the requirement pursuant to Rule 9(b) to plead with specificity").

NIST CSF. The SEC's refusal to engage with the incorporated documents is perhaps most glaring as to its NIST CSF allegations. The NIST Scorecards referenced in the AC make abundantly clear that SolarWinds used NIST CSF to evaluate its cybersecurity posture—which is what "following" the NIST CSF means, as both Defendants and amici have explained. Mot. 23; CISO Br., ECF No. 96, at 9-10. The SEC has no real answer to this, but instead resorts to inapt analogies, arguing that a person cannot "follow" a cake recipe if they skip ingredients or leave the oven off. Opp. 12. The analogy misses the entire point: The NIST CSF is not a set of instructions one must follow like a "recipe." Rather, as the NIST CSF itself takes pains to emphasize, it is a

flexible framework that companies use to evaluate progress against self-defined goals.[6] The SEC's persistent confusion over this issue does not provide a valid basis for its claim. *Cf. Cody v. Conformis, Inc.*, 199 F.Supp.3d 409, 413, 419 (D. Mass. 2016) (finding statement that manufacturing process was "validated" under certain industry protocol was inadequately alleged to be false, where protocol was merely a "framework" providing flexibility in how to "fill in the details," as opposed to being a "foolproof set of specific guidelines").

Moreover, even if the scores the Company gave itself in its NIST CSF self-evaluations were relevant—which they are not, as the Security Statement said nothing about them, and the NIST CSF does not require any minimum scores—the SEC willfully ignores what the NIST Scorecards reflect: The scores were *not*, by any stretch of the imagination, "pervasively low." They instead averaged in the middle of the range *throughout* the Relevant Period, from October 18, 2018 through 2020 (not just "later," as the SEC suggests, Opp. 13). *See* Mot. 24 & Exs. 7-9. The SEC cites low scores "in certain areas," Opp. 13—mostly for *one* particular business segment in an assessment "workbook" *pre-dating the IPO*, ¶¶ 83-88—but the notion that this means that SolarWinds was not following the NIST CSF is both unsupported and absurd.

The SEC's argument regarding the FedRAMP assessment cited in the AC, Opp. 13-14, is even further afield, because the Security Statement did not so much as reference FedRAMP, or the NIST 800-53 controls the SEC believes the assessment was based on. And more broadly, the SEC continues to fundamentally misconstrue this document. First, the assessment itself is expressly

[6] *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity v.1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, at 2-3 (explaining that the CSF provides a "common taxonomy and mechanism" for organizations to "[i]dentify and prioritize opportunities for improvement" and "[a]ssess progress toward the target state"); *id.* at 2 (explaining that the CSF is not "one-size-fits-all" and that organizations "will vary in how they customize practices" described in it); *id.* at 3 ("To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization …. [T]he variety of ways in which the Framework can be used by an organization means that phrases like 'compliance with the Framework' can be confusing and mean something very different to various stakeholders.").

presented as "preliminary," Opp. Ex. 1 at 2, and nowhere does the AC allege that it was ever finalized or approved by anyone with relevant authority. *See In re HealthCare Compare Corp. Sec. Litig.*, 75 F.3d 276, 282-83 (7th Cir. 1996) (dismissing fraud claim based on failure to correct public statement allegedly contradicted by internal memo, where facts alleged were insufficient to show that memo was "certain and reliable" as opposed to "a tentative estimate"). Second, as the controls listed in the document reflect, the assessment related to whether a certain "information system"—*i.e.*, a SolarWinds *cloud product*—could be certified under FedRAMP. That is why the document repeatedly refers to whether "*the* information system" met certain specifications—the term refers to the product at issue.[7] This can be seen even more clearly from portions the SEC omits, which include, among other things, a requirement that "the information system" display a "banner" that users are "accessing a U.S. Government information system."[8] Obviously, that is not something that a system on SolarWinds' own network would do; it applies to a *product* offered to the U.S. Government, which is what this assessment, like all FedRAMP assessments, concerned.[9] Thus, the SEC has no plausible basis to infer from this preliminary, product-specific assessment that there was any pervasive lack of controls across SolarWinds' own network environment.

SDL. As Defendants previously explained, multiple documents cited in the AC reflect the Company had an SDL in place, including the NIST Scorecard the SEC cites showing a score of "2" for the Company's SDL in 2019. Mot. 25. The SEC incorrectly argues that Defendants seek

[7] *See* Opp. Ex. 1 at 5-6 (referring to whether, *e.g.*, "[t]he information system automatically disables inactive accounts after [a certain period]," "[t]he information system automatically audits account creation," and "[t]he information system terminates shared/group account credentials when members leave the group").

[8] *See* Ex. 18, attached to Second Decl. of Serrin Turner. The SEC also omits columns in the spreadsheet referencing the particular cloud products—there were actually four of them—the assessment concerned. *Compare id.* (column headings referencing "Loggly" and "Pingdom" alongside abbreviations for two other products) *with* SolarWinds, *Loggly*, https://www.solarwinds.com/loggly, *and* SolarWinds, *Pingdom*, https://www.solarwinds.com/pingdom.

[9] *See* FedRAMP, *Program Basics*, https://www.fedramp.gov/program-basics (FedRAMP concerns "the adoption and use of cloud services by the federal government").

to draw "an inference … in their favor" from this document. Opp. 16. Rather, Defendants simply pointed out what the cited document actually says, which is that a "2" means that the Company had a "consistent overall approach" to implementing an SDL, even if the approach was mostly "undocumented." Mot. Ex. 9 at 4. That by itself directly contradicts the SEC's allegation that SolarWinds "pervasively failed to follow an SDL during the Relevant Period," ¶ 115. The SEC tries to brush aside this and other glaring inconsistencies between its allegations and its documents, *see* Mot. 25-27, arguing that "[e]xactly how flawed, or non-existent" the SDL was "is a factual dispute," Opp. 16. But it is the SEC's pleading burden to allege a "pervasive failure" with particularity. The SEC cannot evade its pleading burden by making conclusory mischaracterizations of documents and then bracketing those mischaracterizations as a "factual dispute." *See, e.g.*, *Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 146-47 (2d Cir. 2011) (rejecting conclusory allegation contradicted by cited document); *In re PetroChina Co. Ltd. Sec. Litig.*, 120 F.Supp.3d 340, 368 (S.D.N.Y. 2015) (same).

Network Monitoring. The SEC's network monitoring allegations fail for similar reasons. The SEC ignores that the Company's NIST Scorecards reflect that the Company did precisely what the Security Statement said it did as to network monitoring—use "next generation firewalls" to monitor for "network security threats." Mot. 27-28 & Ex. 5. Instead, the SEC cites documents predating the Relevant Period, Opp. 17 (citing ¶¶ 151-52), which themselves only relate to one business segment, ¶ 151, and to controls the Security Statement did not say anything about, ¶ 152. Otherwise, the SEC goes back to mischaracterizing the FedRAMP assessment. The SEC relies on an allegation that the FedRAMP assessment found a gap for a control it quotes as stating: "[t]he organization … [m]onitors information systems for … atypical use … and [r]eports atypical usage of information systems accounts." ¶ 153 (alterations in AC). But this is a misquote of the

document: The quoted control does not reference "information systems" (plural) but rather asks whether the organization "[m]onitors information *system accounts*" and reports atypical use of "information *system accounts*"—the reference being, again, to accounts on *the* "information system," *i.e.*, the cloud product being assessed. *See* Opp. Ex. 1 (listing this among many other controls relating to "*the* information system"). Whether SolarWinds monitored *customer accounts* on a *cloud product* for atypical activity has little to do with monitoring accounts on its own network, much less does it show any pervasive failure in that regard.

Passwords. The SEC's argument regarding the password statement fails at the outset—nowhere did the Security Statement represent that the Company had a "strong" password policy or that its password "best practices" were enforced on every product and system without exception. *Compare* Opp. 18 *with* Mot. Ex. 5. Moreover, the SEC's allegations on their face only reference password issues relating to certain "situations" or certain "systems"—not the Company as a whole. Mot. 29. Again, the SEC must allege "pervasive failures" with particularity. It has not done so.

Access Controls. The SEC does not meet its pleading burden as to access controls either. It states that "SolarWinds broadly granted administrator privileges during the [Relevant Period]," Op. 15, but in trying to substantiate that otherwise vague and unparticularized claim, the AC relies almost exclusively on examples that *predate* the Relevant Period, *see* ¶¶ 181-90. All that remains are: (1) a presentation from December 2018 indicating that work was needed on "the use of local administrator access to nonprivileged users," ¶ 191; (2) a NIST Scorecard from August 2019 with a "1" for "Authentication, Authorization and Identity Management," which did not identify the reason for that score, ¶ 192; and (3) the FedRAMP assessment, which concerned the specific "information system" being assessed, as the SEC's own quotations from the document reflect, ¶ 193-94. None of this provides a plausible basis to conclude that SolarWinds pervasively failed

to implement access controls during the Relevant Period or that any of the specific assertions about access controls in the Security Statement were untrue. *See Constr. Laborers Pension Tr. v. CBS Corp.*, 433 F.Supp.3d 515, 535 (S.D.N.Y. 2020) (rejecting allegations of "pervasive violations" of harassment policy because "handful of examples" did not support that inference).

Further, the SEC fails to explain how its allegations that employees could connect personal devices to the Company's VPN rendered anything in the Security Statement false. The SEC points to the Security Statement's assertion that "access controls 'define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.'" Opp. 15. But not only does the SEC neglect to explain *how* this assertion was supposedly made false by the use of personal devices on the VPN, it also misquotes the Security Statement, which states that "access control *lists*" define user behavior—and the SEC does not explain what, if anything, "access control lists" have to do with the VPN. Mot. Ex. 5. This is not particularized pleading that satisfies Rule 9(b). *See Plymouth Cnty. Ret. Ass'n v. Array Techs., Inc.*, 2023 WL 3569068, at *9 (S.D.N.Y. May 19, 2023) ("Plaintiffs' shotgun approach … falls short of what Rule 9(b) requires: it does not comport with the Second Circuit's exhortation that plaintiffs 'must demonstrate with specificity *why and how*' each statement is materially false or misleading." (emphasis added)).[10]

Blog Posts, Podcasts, and Press Releases. Apart from the Security Statement, the SEC maintains that other statements by Mr. Brown—*e.g.*, that "everything is backed by sound security processes" or that SolarWinds is "commit[ted]" to "high security standards"—are actionable

[10] The SEC's reliance on *In re SolarWinds Corp. Sec. Litig.*, 595 F.Supp.3d 573 (W.D. Tex. 2022) to prop up its Security Statement allegations is unavailing. In that case, private plaintiffs relied on allegations from anonymous witnesses that SolarWinds simply had *no* security team, "*no* password policy," "*no* segmenting of its networks to limit user access," and the like, *id.* at 580 (emphasis added), which were required to be credited on a motion to dismiss. The SEC points to no such witnesses here—indeed, despite taking testimony from numerous individuals, it has not identified a *single* witness who testified to "pervasive" failures or claimed the Security Statement was false or misleading. Rather, the SEC relies on documents incorporated by reference, which, as Defendants have explained, belie any inference that there were pervasive failures to implement the relevant policies in the Security Statement.

because they are "factual." Opp. 22-23. This argument contravenes binding circuit authority rejecting such "vague descriptions" as unactionable puffery. *In Re Philip Morris Int'l Inc. Sec. Litig.*, 89 F.4th 408, 419 (2d Cir. 2023) (statement that clinical trial was "sound" was puffery because it required "subjective assessment"). The SEC seems to suggest that the fact that such statements were made multiple times make them actionable, Opp. 23, but "puffery, no matter how often it is repeated, is still puffery." *Sinanovic v. Wagner Coll.*, 2022 WL 4644238, at *5 (E.D.N.Y. Oct. 1, 2022); *see also Villare v. Abiomed, Inc.*, 2021 WL 4311749, at *15 (S.D.N.Y. Sept. 21, 2021) ("the repetition of puffery does not, by itself, render it actionable"); *cf. In re BHP Billiton Ltd. Sec. Litig.*, 276 F.Supp.3d 65, 79 (S.D.N.Y. 2017), *cited in* Opp. 23 (repeated statements "contained quite specific representations or guarantees of 'some concrete fact or outcome'").

Materiality. The SEC's materiality arguments are also meritless. The SEC fails to meaningfully address SolarWinds' warning in its risk disclosure that the Company was vulnerable to cyberattacks "despite" its security measures. *See* Mot. 33-34 (citing cases); *see also Qudian*, 2019 WL 4735376, at *8 (finding affirmative statements about security controls immaterial where risk disclosures warned the controls "could be breached"). Otherwise, the SEC bizarrely asserts that the stock drop following the 8-K disclosing SUNBURST somehow supports an inference of materiality with respect to the Security Statement. Opp. 21. But the 8-K said *nothing* about SolarWinds' cybersecurity practices or the Security Statement. Mot. Ex. 2. The stock drop was instead obviously a reaction to the attack itself and the resulting "financial, legal, reputational and other risks to SolarWinds" the 8-K described. *Id.* at 5.

B. The SEC Fails to Allege Scheme Liability

The scheme claims must be dismissed because the SEC fails to allege "an inherently deceptive act that was distinct from an alleged misstatement." *In re Turquoise Hill Res. Ltd. Sec. Litig.*, 625 F.Supp.3d 164, 253 (S.D.N.Y. 2022). The SEC's "dissemination" arguments do not

satisfy that requirement. As Judge Liman explained in his well-reasoned decision (which the SEC does not even mention), "distribut[ing]" one's "*own* allegedly false and misleading statements" is not "dissemination." *Id.* at 251-52 (emphasis added). Yet that is what the SEC alleges here: Mr. Brown allegedly both made *and* disseminated the Security Statement. *See, e.g.*, ¶ 58 (alleging "Brown was primarily responsible for creating and approving the Security Statement" and "Brown (or others acting at his direction) disseminated the Security Statement"); ¶ 236 (alleging Mr. Brown was the "maker" of the Security Statement). The SEC cannot base scheme liability on Mr. Brown "disseminating" what are allegedly his own statements.

SolarWinds' public filings provide no basis for scheme liability either. Mr. Brown is only vaguely alleged to have assisted in preparing them, ¶¶ 242, 298, 308, 329, and *Lorenzo* "did not go so far as to create primary liability for 'participation in the preparation' of misstatements," *SEC v. Rio Tinto plc*, 41 F.4th 47, 54 (2d Cir. 2022). Nor do the perfunctory allegations about sub-certifications suffice, Opp. 37. Those sub-certifications are not alleged to have been "externally distributed, examined, or reviewed" and "thus did not 'operate as a fraud or deceit upon any person,' as is required for a deceptive act to support a claim of scheme liability." *In re Washington Prime Grp., Inc. Sec. Litig.*, 2024 WL 1307103, at *28 (S.D. Ohio Mar. 27, 2024). Finally, the SEC's reliance on an employee's alleged misstatement to a customer, Opp. 38, does not suffice to plead an act in furtherance of any scheme to defraud investors, let alone provide a basis for scheme liability for Mr. Brown (who is not alleged to have known about or authorized the statement) or SolarWinds. *See SEC v. Hwang*, 2023 WL 6124041, at *8 (S.D.N.Y. Sept. 19, 2023) (holding that supervising employees who allegedly made misstatements is insufficient for scheme liability).

C. The SEC Fails to Allege a Strong Inference of Scienter

Tellingly, the SEC abandons the scienter theory it trumpeted in the AC—i.e., that Mr. Brown engaged in an intentional "scheme" to conceal the quality of SolarWinds' cybersecurity

practices in order to "obtain and retain business." ¶¶ 5, 46. In lieu of any motive, the SEC now relies solely on a recklessness theory, based on arguments that Mr. Brown knew of information contradicting SolarWinds' public statements. Opp. 38. But the SEC ignores that, in the Second Circuit, "recklessness" requires "a *clear* duty to disclose" and "a *strong* inference of 'conscious recklessness—i.e., a state of mind *approximating actual intent*, and not merely a heightened form of negligence.'" *Setzer v. Omega Healthcare Invs., Inc.*, 968 F.3d 204, 213 (2d Cir. 2020) (emphasis added). The SEC does not and cannot meet this bar.[11]

Risk Disclosure. As to the risk disclosure, the SEC concedes it has not alleged scienter as to the individual *makers* of the statement, instead arguing that Brown's purported knowledge of falsity should be imputed to SolarWinds. Opp. 40. But the SEC has not alleged with requisite particularity what Mr. Brown knew was false or misleading about the risk disclosure. Nor could it, as the SEC acknowledges that Mr. Brown *did not even review* the risk disclosure. ¶ 242; *see City of Omaha Police & Fire Ret. Sys. v. Evoqua Water Techs.*, 450 F.Supp.3d 379, 424 (S.D.N.Y. 2020) (scienter based on non-maker requires "oversight over the public-facing misrepresentation" and "knowledge of the falsity of that statement"); *Hou Liu v. Intercept Pharms., Inc.*, 2020 WL 5441345, at *10 (S.D.N.Y. Sept. 9, 2020) (for imputation, person must be "aware of the allegedly misleading statements").

Nor has the SEC adequately alleged the "connective tissue" between Mr. Brown and the risk disclosure required for imputation. *Hou Liu*, 2020 WL 5441345, at *9. While the SEC vaguely refers to Mr. Brown's signing of sub-certifications and "provi[sion] [of] information to the individuals who drafted" the disclosures, Opp. 40, it fails to describe what information he provided

[11] The SEC fails to plead negligence for similar reasons as it fails to plead scienter, as the alleged facts do not reflect that Mr. Brown should have known that SolarWinds investor filings or the Security Statement were false—even putting the heightened standard of recklessness aside. Mot. 36 n.20.

(or to whom), or how (or even if) that information was used to generate the allegedly misleading statements in the risk disclosures (whatever they are supposed to be). And while the SEC asserts that Mr. Brown was the "principal officer at SolarWinds responsible for cybersecurity practices," Opp. 40, it ignores that he did not in fact hold any officer position during the Relevant Period,[12] and fails to explain how his position connects him to the risk disclosure in any event.

In a sign of desperation, the SEC tacks on a Hail Mary argument that, "even if Brown did not act with scienter regarding the risk disclosures," the SEC has adequately pled "scienter, or collective negligence" by virtue of alleging "widespread corporate failures." Opp. 41. "Collective negligence" is not a concept that appears in securities case law, and the SEC cites no case referring to it. As for collective scienter, the SEC's reliance on that doctrine is unavailing for two reasons. First, it still requires allegations raising "a strong inference that *someone* whose intent could be imputed to the company acted with the requisite scienter," even if the plaintiff lacks enough information to "expressly name[]" such an officer. *Teamsters Loc. 445 Freight Div. Pension Fund v. Dynex Cap. Inc.*, 531 F.3d 190, 195-96 (2d Cir. 2008) (emphasis added). If such a "someone" existed, surely the SEC would have identified them during its three-year investigation. Second, the doctrine only applies where the defendant's statements "grossly" diverged from its "actual" risks, Opp. 41, which cannot be said of the risk disclosure, as it plainly disclosed the risk of cyberattack. Hence, this is not one of the "exceedingly rare instances" of a "dramatic" misstatement where collective scienter may be inferred. *Jackson v. Abernathy*, 960 F.3d 94, 99 (2d Cir. 2020); *see also Rio Tinto plc*, 2019 WL 1244933, at *14 (S.D.N.Y. Mar. 18, 2019).

SUNBURST Disclosure. The SEC's imputation theory fares no better with respect to the

[12] Mr. Brown was Vice-President of Security Architecture throughout the Relevant Period, ¶ 22, reporting to the Chief Information Officer and providing briefings to the Chief Technology Officer. ¶¶ 62, 122, 152. He did not become CISO until after the Relevant Period. ¶ 22.

December 2020 8-K. At most, the SEC alleges Mr. Brown "participated in drafting" and "was responsible" for confirming the accuracy of "technical statements." ¶ 308. But the SEC does not identify the "technical statements" for which Mr. Brown was allegedly responsible, let alone allege that he reviewed or approved the specific language challenged by the SEC. That Mr. Brown was not in any executive position at the time, let alone one with responsibility for disclosures, makes imputation even more dubious. *Jackson*, 960 F.3d at 98.

More fundamentally, the SEC cannot plausibly allege a strong inference of scienter as to the 8-K in the first place—on the part of Mr. Brown or anyone else. The SEC's assertion that the alleged misstatements in the 8-K were intended to "downplay the bad news," Opp. 41, cannot be squared with the Company's voluntarily disclosure of far *worse* news—that up to 18,000 customers were at risk of compromise. Nor can it be squared with the fact that, after the previously disclosed investigation, SolarWinds disclosed the USTP and PAN incidents only four weeks later, which it would not have done if it intended to conceal that information. The statements at issue—that the Company was still investigating whether and to what extent SUNBURST was "successfully exploited" to "infiltrat[e]" any customers, ¶¶ 310-12 —are "more likely explained" by the fact that the Company *actually* sought to investigate the matter, *Iqbal*, 556 U.S. at 680. Even assuming Mr. Brown had already drawn a conclusion on the matter, that fact would not be inconsistent with *the Company* wanting to investigate further. Defendants explained these points, Mot. 38-40, but the SEC has not meaningfully responded to them.

Security Statement. As to the Security Statement, the SEC misconstrues Defendants as simply arguing that SolarWinds' security program "show[ed] progress" during the Relevant Period. Opp. 32. Defendants' argument is that the SEC has not plausibly alleged Mr. Brown ever believed there was any "pervasive failure" to implement the challenged policies in the Security

Statement, which is the SEC's asserted basis for alleging those policies were false. The SEC's own incorporated documents preclude any "strong inference" that Mr. Brown ever held any such belief. For example, the documents allegedly *prepared by Mr. Brown* reflect an understanding that the Company was following the NIST CSF, had an SDL in place, conducted penetration testing of its software, and conducted network monitoring. Mot. 41 & Exs. 7-9. To the extent the documents reflect discrete gaps, that is not enough to infer scienter. *See Lewy v. SkyPeople Fruit Juice, Inc*., 2012 WL 3957916, at *20 (S.D.N.Y. Sept. 10, 2012) (explaining that "repeated or constant" failures to follow policy are needed to establish scienter, and rejecting scienter where facts instead showed that defendants "adhered to, or at least endeavored to adhere to, the announced policy"). Moreover, the SEC has not alleged that Mr. Brown ever "accepted" any views expressed by others in the documents it cites—such as the "preliminary" FedRAMP assessment on which the SEC so heavily (and mistakenly) relies. *See Wochos v. Tesla, Inc.*, 985 F.3d 1180, 1194 (9th Cir. 2021).

Further, the SEC's allegations that Mr. Brown acted with scienter, including the allegations about his allegedly false sub-certifications, cannot be squared with its repeated allegations that Mr. Brown presented information about cybersecurity risks to others at the Company who actually had responsibility for disclosures. *See* ¶¶ 122, 168, 291. That transparent practice belies any "strong inference" of recklessness "approximating actual intent" to deceive. *Setzer*, 968 F.3d at 213. Someone trying to commit (or aid and abet) fraud would not internally broadcast issues they were supposedly trying to conceal. *Jackson*, 960 F.3d at 99 (refusing to impute scienter based on employees who "knew of problems" and escalated them).

II. The Disclosure Controls Claim Should Be Dismissed

The SEC cannot save its disclosure controls claim. The SEC recognizes that SolarWinds' had such controls, in the form of escalation criteria contained in the IRP. Opp. 51. It cannot deny that these criteria were "designed" to ensure that reportable information was timely disclosed.

While the SEC suggests that "just writing out a policy" is not sufficient, *id.*, its allegations show that the IRP did not just exist on paper, but was applied in practice. As alleged, SolarWinds personnel did not ignore the IRP in evaluating the USTP and PAN incidents; they applied it, assigning each incident a classification of "0," to designate an "undetermined" security event. ¶¶ 274, 287; Mot. Ex. 17 at 2. These allegations show that SolarWinds "maintained" the policy, as Rule 13a–15 requires. The SEC merely complains that the IRP was applied erroneously. Opp. 51.

That theory does not support a disclosure controls claim, for two reasons. First, it is based on a hindsight-driven view of what SolarWinds security personnel *should* have concluded about the incidents, rather than what they actually believed at the time. This is not a "factual dispute[]," Opp. 34, but a deficiency of the SEC's allegations. The SEC alleges that, based on similarities between the USTP and PAN incidents, SolarWinds and Brown "knew, or were reckless or negligent in not knowing, that the Company's systems had been breached" and that this (unidentified) breach somehow caused both incidents. ¶ 280. But the SEC alleges no facts implying anyone at SolarWinds actually "knew" the Company had been "breached" and failed to escalate it. Indeed, this conclusory assertion is contradicted by allegations in the AC acknowledging SolarWinds was not able to "uncover the root cause" of either incident. ¶¶ 270, 284; *see Adeghe v. Procter & Gamble Co.*, 2024 WL 22061, at *4 (S.D.N.Y. Jan. 2, 2024) (court need not credit statements contradicted by other allegations in a complaint). The SEC alleges no facts to support an inference that anyone *should have known* this at the time either, but it does not matter: employees could only apply the IRP to what they *actually* knew. And because they did not know the root cause of either incident, it was reasonable for them to classify each as "undetermined."

Second, even if this classification could be deemed an error, whether reckless, negligent, or otherwise, that would not establish a disclosure controls violation. Rule 13a–15 only required

SolarWinds to maintain disclosure controls "designed"—not "guaranteed"—to ensure timely reporting. The SEC flatly misstates the applicable requirement when it insists that Rule 13a–15 "requires that an issuer's [disclosure] policies be 'effective.'" Opp. 50. It cites only to a subsection requiring management to regularly "*evaluate* … the effectiveness of the issuer's disclosure controls," 17 C.F.R. § 240.13a–15(b). That subsection does not purport to establish a strict liability regime requiring disclosure controls to be effective at all times. Moreover, the SEC's disclosure controls claim is not brought under subsection (b) of Rule 13a–15, but is brought under subsection (a), ¶¶ 360-66, which merely requires controls "*designed* to ensure" that reportable information is timely reported. The SEC alleges no facts showing that SolarWinds failed to meet *that* standard.[13]

III. The Internal Accounting Controls Claim Should Be Dismissed

The SEC's arguments on internal accounting controls ignore the statutory text and legislative history, and only confirm it is trying to extend the law far beyond its intended bounds.

The SEC complains that Defendants place too much weight on the term "accounting," Opp. 44, but all of the controls described in Section 13(b)(2)(B) must be construed in relation to accounting, as "accounting controls" are what the statute is expressly about. Subsection (iii)'s reference to "accounting controls" designed to restrict "access to assets" is no exception. It refers to controls designed to restrict access to assets so as to *prevent or detect accounting discrepancies—i.e.*, to ensure assets are properly *accounted* for. This construction is bolstered by the next subsection, which requires companies to have controls to regularly check accounting of assets against existing assets and to address any discrepancies. 15 U.S.C. § 78m(b)(2)(B)(iv). In

[13] Courts have likewise rejected the alleged misapplication of internal controls as a basis for a securities fraud claim where a company has stated that it maintains such controls. *See* Mot. 45 (collecting cases). The SEC tries to brush these cases aside because they were not brought directly under Rule 13a–15, Opp. 53, but their logic applies equally to Rule 13a–15. The SEC is unable to cite a single case supporting its inflated view of Rule 13a–15, and Defendants are unaware of any case finding a violation where the disclosure controls were properly designed but merely alleged to have been applied erroneously.

other words, subsection (iii) requires assets to be secured so that companies can accurately count them, and subsection (iv) requires them to be regularly counted.

Legislative history confirms this construction. As the SEC acknowledges, Section 13(b)(2)(B)(iii) derives from the AICPA Statement on Auditing Standards No. 1 ("SAS 1")—specifically its concept of "safeguarding assets." Opp. 45. But the SEC ignores that SAS 1 specifically rejects a "broad interpretation" of this concept to mean "protection against something undesirable" happening to a company's assets. SAS 1 §§ 320.14 (proposing this interpretation) & 320.19 (rejecting it). Instead, SAS 1 explains the concept "refers only to protection *against loss*" of assets—like "physical loss of assets such as cash, securities, or inventory," which could result in accounting errors or irregularities as to those assets. *Id.* § 320.15 (emphasis added); *see also id.* § 320.36 (explaining that "[a]nyone who … has access to assets ordinarily is in a position to perpetrate errors or irregularities," such as issuing a company check without recording it).[14]

This is why the SEC's reliance on Section 13(b)(2)(b)(iii) is so misguided. The controls at issue have nothing to do with preventing accounting discrepancies due to loss of assets, but instead concern protecting the Company's network and software from cyberattacks. The SEC's assertion that SolarWinds' software products are in certain ways "assets" of the Company, Opp. 49-50, misses the point: The controls do not relate to preventing the *loss* of these "assets." Indeed, software products are not even *capable* of being "lost" like "cash, securities, or inventory" are. For

[14] The SEC attacks a strawman in arguing that "'the accounting provisions of the FCPA are not exclusively concerned with the preparation of financial statements.'" Opp. 44 (quoting *Promotion of the Reliability of Financial Information and Prevention of the Concealment of Questionable or Illegal Corporate Payments and Practices*, Rel. No. 34-15570, 1979 WL 173674, at *6 (SEC Feb. 15, 1979)). The quoted document simply notes that, in addition to ensuring accurate financial statements, robust accounting controls serve to prevent corrupt diversion of corporate assets. *See* 1979 WL 173674, at *6 (explaining statute was designed to "prevent off-the-books slush funds" and ensure "proper accounting of the use of corporate funds"). No one disputes that the aims of Section 13(b)(2)(B) extended to corporate corruption—that is why it was enacted as part of the Foreign Corrupt Practices Act—but the point is that the *means* Congress prescribed in service of those aims were *accounting* controls, not any other type of controls.

example, the SEC cites the Company's SDL as an "internal accounting control," Opp. 43, but the SDL serves to prevent software products from being *hacked*, not "lost." A hack may be "something undesirable," but it does not mean the software vanishes from the Company's inventory, or that it would be error to continue listing the underlying technology as an intangible asset on the Company's books.[15]

The two cases the SEC relies upon do not help its position. Each concerns a lack of controls to ensure that a company's inventory or cash is properly accounted for. *SEC v. World-Wide Coin Investments, Ltd.* involved a rare-coin company whose vault "was unguarded and left open all day to all employees," which made it impossible for "the accountant" to determine "[a]n accurate valuation of World-Wide's inventory." 567 F.Supp.724, 738 (N.D. Ga. 1983). The court found an internal accounting controls violation on this basis, *id.* at 752, explaining that "[i]nternal controls safeguard assets and assure the reliability of financial records, one of their main jobs being to *prevent and detect errors and irregularities that arise in the accounting systems* of the company." *Id.* at 750 (emphasis added). In the other case, *SEC v. Cavco Industries*, the defendant company gave its CEO broad authority to invest its surplus cash in stocks of his choosing, which he used to engage in insider trading. 2022 WL 1491279, at *1 (D. Ariz. 2022). The internal accounting controls violations concerned the lack of controls over what CEO could do with the company's cash: "there were insufficient checks for how investments outside [the company's insider trading policy] would be identified and reported and for how improper investments would be prevented." *Id.* at *3. Thus, there too the concern was ultimately about cash walking out the door without sufficient oversight—a concern with a discernable nexus to *accounting*.

[15] For similar reasons, the SEC's analogy to Ford trucks, Opp. 49, is off-base. No one would argue that a defect in Ford's quality control procedures that caused its trucks to have a safety issue would constitute a failure of "internal accounting controls." But that is the implication of the SEC's argument here that SolarWinds' SDL—designed to prevent bugs in software—constitutes an "internal accounting control."

Nor does the SEC have any persuasive response to Defendants' cases, all of which emphasize that internal accounting controls ultimately must concern "accounting." The SEC asserts the cases did not specifically concern subsection (iii) of Section 13(b)(2)(B), Opp. 47-48, but the point is that *all* the statute's subsections fall under the umbrella of "internal *accounting* controls" and must be interpreted in that light. Reading subsection (iii) to apply here would strip the provision of any link to accounting concerns and give the SEC undefined and unbounded authority to substantively regulate the *cybersecurity* controls of public companies. Such an acontextual reading of the statute finds no support in either caselaw or common sense.

IV. The Aiding-and-Abetting Claims Should Be Dismissed

The SEC's aiding-and-abetting claims add nothing legally or logically to its case. *See* Br. 49-50. They are based on the exact same alleged conduct as the primary violations (and nothing more), and must be dismissed along with them. Moreover, the SEC cannot explain how its theory satisfies even the first element of aiding and abetting: "the existence of a securities law violation by the primary (*as opposed to the aiding and abetting*) party." *SEC v. Apuzzo*, 689 F.3d 204, 211 (2d Cir. 2012) (emphasis added). Despite the SEC's characterization, *Lorenzo v. SEC* does suggest otherwise when it notes that "the same conduct [can] be a primary violation with respect to one offense and aiding and abetting *with respect to another* [*offense*]." 587 U.S. 71, 83 (2019) (emphasis added); *cf. SEC v. Farnsworth*, 2023 WL 5977240, at *20 (S.D.N.Y. Sept. 14, 2023) (requiring conduct "in addition to making [the defendant's] own material misstatements" to satisfy the "substantial assistance" element). In fact, the Second Circuit rejected the SEC's "overreading [of] *Lorenzo*" precisely because it would "muddle primary and secondary liability," *Rio Tinto*, 41 F.4th at 55, as the SEC's aiding-and-abetting theory would do here.

CONCLUSION

The Amended Complaint should be dismissed in its entirety, with prejudice.

Dated: May 3, 2024

Respectfully submitted,

/s/ Serrin Turner

Serrin Turner
Nicolas Luongo
LATHAM & WATKINS LLP
1271 Avenue of the Americas
New York, NY 10020
Telephone: (212) 906-1200
Facsimile: (212) 751-4864
serrin.turner@lw.com
nicolas.luongo@lw.com

Sean M. Berkowitz (*pro hac vice*)
Kirsten C. Lee (*pro hac vice*)
LATHAM & WATKINS LLP
330 N. Wabash, Suite 2800
Chicago, IL 60611
Telephone: (312) 876-7700
Facsimile: (617) 993-9767
sean.berkowitz@lw.com
kirsten.lee@lw.com

Michael Clemente (*pro hac vice*)
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
Telephone: (202) 637-2200
Facsimile: (202) 637-2201
michael.clemente@lw.com

Counsel for Defendants SolarWinds Corp. and Timothy G. Brown